BUNDESREPUBLIK DEUTSCHLAND

Bescheinigung

Die Anmelderin International Business Machines Corp. in Armonk, N.Y./V.St.A. hat eine Patentanmeldung unter der Bezeichnung

"Verfahren und Vorrichtung zur Zugangskontrolle zu Inhalten von Web-Seiten unter Verwendung eines mobilen Sicherheitsmoduls"

am 19. August 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole H 04 L und G 06 F der Internationalen Patentklassifikation erhalten.

München, den 27. März 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Ebert

Aktenzeichen: 199 39 281.1

B E S C H R E I B U N G

Verfahren und Vorrichtung zur Zugangskontrolle zu Inhalten von Web-Seiten unter Verwendung eines mobilen Sicherheitsmoduls

Die vorliegende Erfindung beschreibt ein Verfahren und eine Vorrichtung zur Zugangskontrolle zu Inhalten von Web-Seiten unter Verwendung von mobilen Sicherheitsmodulen, insbesondere Chipkarten.

Das Internet, d.h. das World Wide Web, ist zu einem neuen Informations- und Geschäftsmedium geworden. Die zunehmende Kommerzialisierung des Internets führt zu ständig neuen Geschäftsideen, die über das Internet abgewickelt werden. Der Internet-Benutzer kann schon heute nahezu alle Geschäfte des täglichen Lebens über das Internet abwickeln. Auch in der Geschäftswelt hat das Internet einen nicht mehr wegzudenkenden Platz gefunden. Firmen nutzen das Internet sowohl bei der Entwicklung als auch beim Vertrieb ihrer Produkte.

Diese Möglichkeiten des Internets bergen jedoch auch Gefahren. Über das Internet werden zunehmend auch vertrauliche Informationen zwischen Client und Server ausgetauscht. Dies gilt insbesondere beim Austausch von geheimem Know-How. Der Client und der Server müssen daher sicher sein, dass kein Zugriff auf die vertraulichen Informationen während der Übertragung über das Internet möglich ist. Darüber hinaus muß auch sichergestellt sein, dass die Authentizität des Empfängers der vertraulichen Information gewährleistet ist. Schließlich gehen auch immer mehr Anbieter von Web-Servern dazu über, den Zugang zu Webinhalten einzuschränken, d.h. den Zugriff nur gegen Eingabe von UserID und Paßwort zuzulassen. Im Stand der

Technik haben sich einige Verfahren etabliert, die sicherstellen, dass die Authentizität zwischen Client und Server gewährleistet ist und dass kein unberechtigter Zugriff während der Übertragung möglich ist.

Stand der Technik

Soweit der Zugriff auf die Web-Seiten mittels einer UserID und eines Paßworts beschränkt ist, wird dies dem Browser mitgeteilt und der Browser eröffnet ein Dialogfenster zur Eingabe einer UserID und/oder eines Paßworts. Nach Eingabe der UserID und des Paßworts sendet der Browser die Eingabe an den Web-Server, die bei Richtigkeit den Zugriff auf die Web-Seiten eröffnet.

Ein Nachteil dieses Verfahrens liegt in der Vergabe und der Verwaltung der UserIDs und der Paßwörter und der dadurch bedingten Möglichkeit, dass die UserIDs und die Paßwörter durch Nichtberechtigte mißbraucht oder bei ihrer Übertragung vom Client zum Web-Server abgehört werden können.

In einem verbesserten Verfahren speichert der Web-Server die TCP/IP-Adresse des Clients in einer Tabelle. Die TCP/IP Adresse gilt damit als authorisiert. Ein Nachteil dieses Verfahrens liegt darin, dass die TCP/IP Adresse des berechtigten Clients durch eine andere TCP/IP Adresse eines nichtberechtigten Clients ersetzt werden kann, wenn der nichtberechtigte Client die UserID und das Paßwort ausgespäht hat. In diesem Fall erhält der Nichtberechtigte dennoch Zugriff zu dem Web-Server.

Das SSL (Secure Socket Layer) ist ein Übertragungsprotokoll zur sicheren Übertagung von Informationen. Heutige Browser unterstützen weitgehend dieses Protokoll. Browser, die das SSL unterstützen, enthalten eine Datenbank mit Zertifikaten

für öffentliche Schlüssel. Jeder öffentliche Schlüssel wird durch ein Zertifikat von einer anerkannten Zertifizierungsstelle zertifiziert. Der zugangsgeschützte Web-Server enthält einen privaten Schlüssel, dem jeweils ein öffentlicher Schlüssel zugeordnet ist. Für diesen öffentlichen Schlüssel existiert auf dem Web-Server ebenfalls ein Zertifikat.

Der Web-Server sendet dem Client das Zertifikat. Das Zertifikat besteht aus dem öffentlichen Schlüssel, Identitätsdaten und einer Signatur. Die Signatur wurde vom Web-Server mittels des privaten Schlüssels erstellt. Der Client überprüft die Gültigkeit des Zertifikats anhand der abgespeicherten Zertifikate und generiert mittels eines Verschlüsslungsalgorithmus und des öffentlichen Schlüssels eine Signatur. Stimmt die Signatur im Zertifikat mit der generierten Signatur überein, hat sich der Server authentifiziert.

Das gleiche Verfahren kann auch zur Authentifizierung des Clients angewandt werden.

Voraussetzung ist auch hier, dass der Client einen privaten Schlüssel und ein Zertifikat benötigt.

Der private Schlüssel muß gegen Zugriff geschützt sein. Daher darf der private Schlüssel nicht auf die Festplatte des Clients abgelegt werden. Alternativ hierzu kann der private Schlüssel auf eine Karte gebracht werden. Nachteilig ist jedoch, dass die Karte in der Lage sein muß, ein Public-Key-Verfahren durchzuführen. Hierzu benötigt die Karte einen kryptografischen Co-Prozessor. Dies macht die Karte jedoch teuer.

Um einen sicheren Nachrichtenweg herzustellen, bietet das SSL Protokoll die Möglichkeit zur Verschlüsselung der zu

übertragenden Informationen über einem Session-Key, auf den sich der Client und der Web-Server geeinigt haben. Der Session-Key ist ein symmetrischer Schlüssel. Er wird verwandt, um die zu übertragenden Informationen zu verschlüsseln.

Aufgabe der vorliegenden Erfindung ist ein Verfahren und eine Vorrichtung bereitzustellen, das die dargestellten Nachteile des Standes der Technik zur Authentifizierung zwischen Client und Server vermeidet.

Diese Aufgabe wird durch die Merkmale in Anspruch 1,15,17,18 und 20 gelöst. Weitere vorteilhafte Ausführungsformen der vorliegenden Erfindung sind in den Unteransprüchen niedergelegt.

Die wesentliche Vorteil der vorliegenden Erfindung liegt darin, dass die erfinderische Zugangskontrolle zu Web-Seiten keine Änderung der bereits existierenden Browser erfordert. Durch den Einsatz einer Chipkarte wird auch die Sicherheit des hier angewandten Authentifizierungsverfahrens erhöht.

Die vorliegende Erfindung wird anhand eines bevorzugten Ausführungsbeispiels anhand Figuren beschrieben, wobei

FIG.1 die Komponenten zeigt, die der vorliegende Erfindung zugrunde liegen

FIG.2 das erfinderische Verfahren zur Authentifizierung und Zugangskontrolle

FIG.1 zeigt die Komponenten zur Durchführung der vorliegenden Erfindung. Auf der Client-Seite ist ein Datenverarbeitungsgerät mit einem Browser, ein Kartenleser und ein mobiles Sicherheitsmodul, z.B. Chipkarte,

installiert. Der Browser ist in der Lage HTML-Seiten darzustellen und Applets in seiner virtuellen Maschine (JVM-Java Virtuell Machine) auszuführen. Applets sind Programme in der Programmiersprache Jave, die vom Web-Server zusammen mit der Web-Seite geladen werden. Die Applets haben die Funktion mit der Chipkarte zu kommunizieren, z.B. über die APDUs (Application Protocol Data Units). Das Applet benötigt eine Programmbibliothek, um mit der Karte zu kommunizieren. Dies ist deshalb erforderlich, weil die Kommunikation nicht zur Standardfunktionalität des Browsers gehört. Die Chipkarte muß in der Lage sein, mittels eines Schlüssels eine kryptografische Prüfsumme zu berechnen oder eine digitale Signatur zu generieren. Der Schlüssel liegt in einem geschützten Bereich der Chipkarte. Darüber hinaus ist auf der Karte vorzugsweise die individuelle Kartennummer abgelegt.

Auf der Server-Seite ist ein Web-Server oder Datenverarbeitungsgerät, der HTTP-Requests vom Client (HTTP-Server) bedienen kann. Der Server ist zusätzlich in der Lage neben statischen HTML-Seiten auch Programme (CGI-Common Gateway Interface) oder Servlets aufzurufen. Servlets sind in Java geschriebene Programme, die auf Web-Servern zum Einsatz kommen. In der vorliegenden Erfindung haben die Servlets die Funktion, die von der Client-Seite erzeugte kryptografische Prüfsumme (digitale Signatur) zu verifizieren und damit die Authentizität des Clients gegenüber dem Web-Server sicherzustellen.

Der Web-Server kann einen geschützten Bereich aufweisen, der nur über eine Zugriffskontrolle zugreifbar ist und einen nicht geschützten Bereich aufweisen, auf den ohne Zugriffskontrolle zugegriffen werden kann.

Client und Web-Server sind über eine Datenverbindung, z.B. Internet oder Intranet, verbunden und kommunizieren über ein Standardübertragungsprotokoll, z.B. TCP/IP.

Um die Sicherheit des erfinderischen Verfahrens gegen Abhören weiter zu erhöhen, wird SSL (Secure Sockets Layer) als Übertragungsprotokoll vorgeschlagen.

In FIG.2 wird der Ablauf des erfinderischen Verfahrens zur Zugangskontrolle auf geschützte Web-Seiten eines Web-Servers näher beschrieben. Das erfinderische Verfahren enthält folgende Verfahrensschritte:

1. Client fordert über die Eingabe einer URL (Uniform Resource Locator) eine geschützte Web-Seite auf einem Web-Server (HTTP-Request für Seite X). Durch die Anforderung des Clients wird auf dem Web-Server ein Servlet gestartet. Das Servlet prüft anhand einer Liste, ob die URL als Parameter eine gültige Session ID enthält. Eine SessionID ist eine Zugriffsvoraussetzung zum Zugriff auf eine geschützte Web-Seite. Ist die SessionID in der Liste enthalten, wird unter Punkt 10 näher beschrieben. Ist sie nicht enthalten (initialer Kontakt) beginnt die Authentifizierung nach Schritt 2.

2. Das Servlet schickt dem Client eine Authentifizierungs-Seite, welche ein Authentifizierungs-Applet enthält. Dieses Authentifizierungs-Applet ist parametrisiert mit einer Zufallszahl, welche vom Servlet erzeugt worden ist, und der URL-Adresse der ursprünglich angeforderten Seite (HTTP-Request für Seite X). Das Authentifizierungsapplet wird vorzugsweise im flüchtigen Speicher des Clients abgelegt und vom Browser zur Ausführung gebracht bzw. aktiviert.

3. Das Applet fordert den Benutzer zum Ausweisen mittels Chipkarte auf startet eine Kommunikation mit der Chipkarte

vorzugsweise über APDUs. Das Applet sendet die Zufallszahl zur Chipkarte.

4. Die Chipkarte berechnet aus der Zufallszahl und der Kartennummer mittels eines Schlüssels, der auf der Chipkarte im geschützten Bereich abgelegt ist, eine kryptografische Prüfsumme oder digitale Signatur. Die Prüfsumme/digitale Signatur und die Kartennummer werden an das Applet zurückgegeben.

5. Das Applet baut dann eine Kommunikation zum Servlet auf dem Web-Server auf und reicht diese Daten an das Servlet.

6. Das Servlet prüft, ob die kryptografische Prüfsumme/ Signatur unter Verwendung eines zur Chipkarte passenden Schlüssels. Beim symmetrischen Verschlüsselungsverfahren ist das Servlet im Besitz des gleichen Schlüssels; beim asymmetrischen Verschlüsselungsverfahren ist das Servlet im Besitz des öffentlichen Schlüssels.

a) bei Nichtübereinstimmung der Prüfsumme sendet das Servlet eine negative Antwort an das Applet. Das Applet zeigt dem Benutzer eine Fehlermeldung.

b) bei Richtigkeit der Prüfsumme generiert das Servlet eine eindeutige SessionID aus einem großen Wertebereich, um ein gezieltes Herausfinden durch einen Unberechtigten zu vermeiden.

Die SessionID wird mit vorzugsweise mit einem Verfallsdatum versehen und in die Liste der gültigen SessionID des Servlet eingetragen. Die SessionID weist diesen Benutzer für alle Requests innerhalb der Session als berechtigten Benutzer aus. Die SessionID verliert ihre Gültigkeit bei:

- Ablauf einer festgelegten Zeit

- Sitzungsbeendigung durch Logoff Seite

7. Die SessionID wird vom Servlet an das Applet übertragen. Vorzugsweise wird vom Applet die erfolgreiche Authentifizierung bestätigt.

8. Das Applet verfügt nach dem Abschluss des Verfahrensschritt 7 über folgende Informationen:

- die ursprünglich angeforderte URL Adresse für Seite X aus Schritt 3
- die SessionID aus Schritt 7

Aus diesen Informationen generiert das Applet eine neue URL, wobei die neue URL aus der ursprünglichen Adresse und der SessionID besteht, und übergibt diese an den Browser. Die Funktion des Applets ist damit erschöpft.

9. Der Browser fordert die betreffenden Web-Seite vom Web-Server an.

10. Die Anforderung der Seite X führt zum Aufruf des Servlets im Server. Das Servlet prüft, wie in Schritt beschrieben, das Vorhandensein der SessionID in der URL. Bei Vorhandensein der SessionID überprüft das Servlet, ob die SessionID in der Liste enthalten und im Falle, dass sie enthalten ist, ob ein eventuell vorhandenes Gültigkeitsdatum abgelaufen ist.

Sind alle Zugriffsvoraussetzungen erfüllt, wird die adressierte Web-Seite in den Speicher des Web-Servers geladen und aufbereitet. Bei der Aufbereitung wird die entsprechende Web-Seite nach Links zu anderen Web-Seiten innerhalb des geschützten Zugangsbereichs durchsucht. Werden solche Links gefunden, werden sie um die SessionID des Benutzers ergänzt. Vorzugsweise wird am Ende der

aufgerufenen Seite ein zusätzlicher Link zum Beenden der Session eingefügt, welcher ebenfalls die SessionID enthält (siehe 13).

11. Servlet überträgt die Seite mit den modifizierten Links an den Client.

12. Folgt der Benutzer einem Link auf der angezeigten Seite, der wiederum in den geschützten Bereich verweist, enthält dieser Link bereits die zur Authentifizierung notwendige SessionID und damit wird diese Seite ohne erneute Authentifizierung nach Schritt 2ff zum Client übertragen.

13. Eine explizite Beendigung der Session mit dem Verlust der SessionID erfolgt durch:

- Anwahl des Links zum Logoff (siehe Schritt 10)
- Ablauf der Zeit, für die eine SessionID vergeben worden ist.

14. Servlet erhält den Logoff-Request von Schritt 13 und löscht die im Logoff-Request enthaltene Session aus der Liste der gültigen SessionIDs. Vorzugsweise bestätigt das Servlet dem Benutzer die Beendigung der Sitzung.

A N S P R Ü C H E

1. Verfahren zur Zugangskontrolle zu geschützten Inhalten auf einem Server, wobei das Verfahren folgende Komponenten voraussetzt:

   a) einen Server
   b) einen Client
   c) ein Lesegerät für ein mobiles Sicherheitsmodul
   d) ein Sicherheitsmodul mit zumindest einem geschützten Bereich zur Speicherung eines Schlüssels
   e) eine Datenleitung zur Kommunikation zwischen Client und Server

   gekennzeichnet durch folgende Schritte:

   aa) Senden eines Request an den Server zum Abrufen von zugriffsgeschützten Inhalten

   bb) Senden eines Authentifizierungsmoduls vom Server an den Client zur Ausführung im Client

   cc) Durchführen eines Authentifizierungsprotokolls zur Authentifizierung des mobilen Sicherheitsmoduls und gegebenenfalls seines Inhabers mittels des Authentifizierungsmoduls

   dd) Ergänzen des Requests nach Schritt aa) durch eine Session ID die im Laufe der Kommunikation zwischen Authentifizierungsmodul und Server generiert worden ist, wenn die Authentifizierung nach Schritt cc) Erfolg hatte

ee) Senden des neuen Requests an die Server-Anwendung

ff) Überprüfen der SessionID im Request auf Registrierung im Server

gg) Aufbereiten des angefragten Inhalts zum Übertragen und Durchsuchen des Inhalts nach weiteren Links zu anderen zugriffsgeschützten Inhalten

hh) Ergänzen der identifizierten Links um die SessionID

ii) Senden des nach des Schritt hh) modifizierten Inhalts an den Client.

2. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass der Server ein Web-Server ist und dass die geschützten Inhalte Web-Seiten darstellen, die durch einen URL - Request von einem Client über einem Browser aufgerufen werden.

3. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass das Authentifizierungsprotokoll nach folgenden Schritten erfolgt:

jj) Generieren einer Zufallszahl durch die Server-Anwendung, wenn der angefragte Inhalt zugriffsgeschützt ist und die Zugriffsvoraussetzungen zum Zugriff nicht erfüllt sind, und Senden der Zufallszahl an das Authentifizierungsmodul

kk) Senden der Zufallszahl von dem Authentifizierungsmodul an das mobile Sicherheitsmodul

ll) Generieren einer digitalen Signatur unter Berücksichtigung der Identifikationsnummer des mobilen Sicherheitsmoduls, der Zufallszahl und dem Schlüssel des mobilen Sicherheitsmoduls im mobilen Sicherheitsmodul

mm) Senden der digitalen Signatur zum Server

nn) Überprüfen der Richtigkeit der digitalen Signatur unter Verwendung eines Sicherheitmoduls des Servers.

4. Verfahren nach Anspruch 2 dadurch gekennzeichnet, dass die Server-Anwendung ein Servlet und das Client-Authentifizierungsmodul ein Authentisierungsapplet ist und dass beim Empfang eines URL-Requests das Servlet den URL-Request auf Vorhandensein einer SessionID überprüft und beim Fehlen einer Session ID ein Authentisierungsapplet mit einer Zufallszahl an den Client sendet.

5. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass die Kommunikation zwischen Client und Server über SSL (Secure Sockets Layer) als Übertragungsprotokoll erfolgt.

6. Verfahren nach Anspruch 4 dadurch gekennzeichnet, dass das Authentifizierungsapplet mit dem Servlet über das TCP/IP-Protokoll über Internet oder Intranet kommuniziert.

7. Verfahren nach Anspruch 3 dadurch gekennzeichnet, dass die digitale Signatur über einen symmetrischen Kryptoalgorithmus mit Hilfe eines geheimen Schlüssels, der zwischen Client und Server vereinbart ist, oder

über einen asymmetrischen Kryptoalgorithmus mit Hilfe eines privaten Schlüssels erfolgt, wobei der Server im Besitz des öffentlichen Schlüssels ist.

8. Verfahren nach Anspruch 7 dadurch gekennzeichnet, dass der symmetrische Kryptoalgorithmus DES oder Trible-DES und der asymmetrische Kryptoalgorithmus RSA, DSA oder ein Eliptic-Curve-Algorithmus ist.

9. Verfahren nach Anspruch 4 dadurch gekennzeichnet, dass das Servlet bei Nichtübereinstimmung der digitalen Signatur eine Fehlermeldung an das Client-Applet sendet.

10. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass das Erzeugen einer SessionID aus einem großem Wertebereich erfolgt, um ein gezieltes Herausfinden zu verhindern.

11. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass die SessionID den Benutzer für alle Requests innerhalb einer definierten Session als Berechtigter ausweist.

12. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass die SessionID mit einer Gültigkeitsdauer versehen ist.

13. Verfahren nach Anspruch 12 dadurch gekennzeichnet, dass die SessionID ihre Gültigkeit bei Ablauf einer festgelegten Zeit oder bei Sitzungsbeendigung durch Logoff-Seite verliert.

14. Verfahren nach Anspruch 1 dadurch gekennzeichnet, dass die nach Schritt dd) erzeugte SessionID in einer Tabelle registriert wird und dass das Vorhandensein einer Eintragung in der Tabelle als

Zugriffsvoraussetzung für alle zugangsgeschützten Web-Seiten ist.

15. Verfahren nach Anspruch 14 dadurch gekennzeichnet, dass bei Ablauf der Gültigkeit der SessionID oder bei Sitzungsbeendigung durch Logoff-Seite die SessionID in der Tabelle wieder gelöscht wird.

16. Vorrichtung zumindest enthaltend folgende Komponenten:

a) Client zumindest enthaltend:
aa) einen Browser
bb) ein Computerprogrammprodukt zur Ausführung der Verfahrensschritte aa), cc), dd), ee) nach Anspruch 1
cc) Lesegerät für das mobile Sicherheitsmodul

b) Server enthaltend zumindest:
aa) ein Computerprogrammprodukt zur Ausführung der Verfahrensschritte bb), ff), gg), hh) und ii) nach Anspruch 1

c) eine Kommunikationsverbindung zwischen Client und Server

17. Vorrichtung nach Anspruch 16 dadurch gekennzeichnet, dass der Server ein Web-Server ist und dass die Kommunikationsverbindung zwischen Client und Web-Server über das Internet oder Intranet erfolgt.

18. Web-Server zumindest enthaltend:

a) einen nichtflüchtigen Speicher zur Speicherung von Web-Seiten

b) ein Computerprogrammprodukt zur Ausführung der Verfahrensschritte bb), ff), gg), hh) und ii) nach Anspruch 1.

19. Web-Server nach Anspruch 18 dadurch gekennzeichnet, dass ein Sicherheitsmodul zur Durchführung des Verfahrensschritts nn) nach Anspruch 1 zusätzlich angeordnet ist.

20. Client zumindest enthaltend:
aa) einen Browser
bb) ein Computerprogrammprodukt zur Ausführung der Verfahrensschritte aa), cc), dd), ee) nach Anspruch 1.

21. Client nach Anspruch 20 weiter enthaltend:
a) Chipkartenlesegerät für ein mobiles Sicherheitsmodul
b) Chipkarte mit einem nichtflüchtigen, geschützten Speicher zumindest enthaltend:
aa) Kartennummer
bb) kryptografischer Schlüssel.

22. Computerprogrammprodukt, das im internen Speicher eines digitalen Rechners gespeichert ist, enthaltend Teile von Softwarecode zur Ausführung des Verfahrens nach Anspruch 1-15, wenn das Produkt auf dem Rechner ausgeführt wird.

Z U S A M M E N F A S S U N G

Die vorliegende Erfindung beschreibt eine Vorrichtung und ein Verfahren zur Zugangskontrolle zu geschützten Web-Seiten eines Web-Servers unter Verwendung eines Authentifizierungsverfahrens. Das erfinderische Verfahren gliedert sich in ein allgemeines Verfahren zur Authentifizierung des Clients und einem nachgeschalteten Verfahren zur Erteilung der Zugriffsberechtigung auf die geschützen Web-Seiten unter Generierung einer SessionID, die dem Client nach erfolgreicher Authentifizierung mitgeteilt wird, und Hinzufügung der SessionID als Bestandteil des neuen Requests. Hierbei wird sichergestellt, dass auch die Links der zugriffsgeschützten Web-Seite erfaßt und mit einer SessionID als Zugriffsberechtigung versehen werden. Die SessionID ist vorzugsweise mit einem Gültigkeitsdatum versehen. Die vorliegende Erfindung paßt sich in die bereits existierende Browser-Infrastruktur ein, ohne dass hierzu Änderungen notwendig sind. Durch die Verwendung einer Chipkarte wird die Sicherheit des Authentifizierungsverfahrens erhöht.

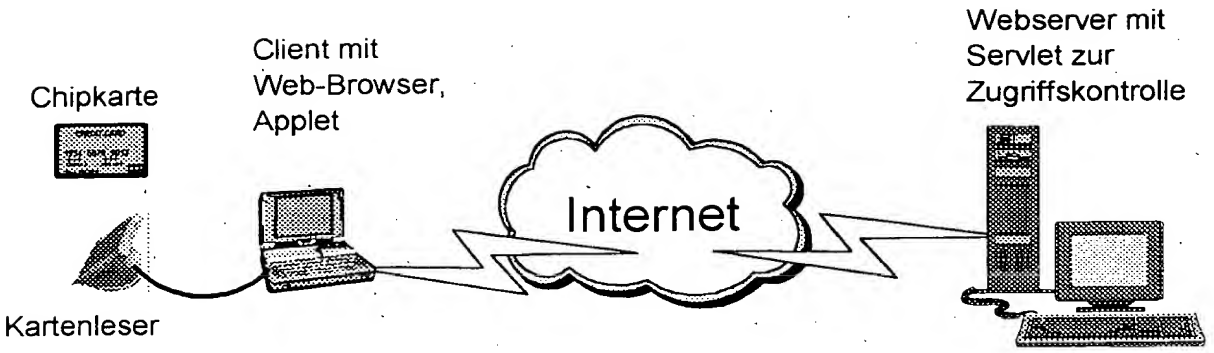
Chipkarte
Client mit
Web-Browser,
Applet
Webserver mit
Servlet zur
Zugriffskontrolle
Internet
Kartenleser

FIG. 1

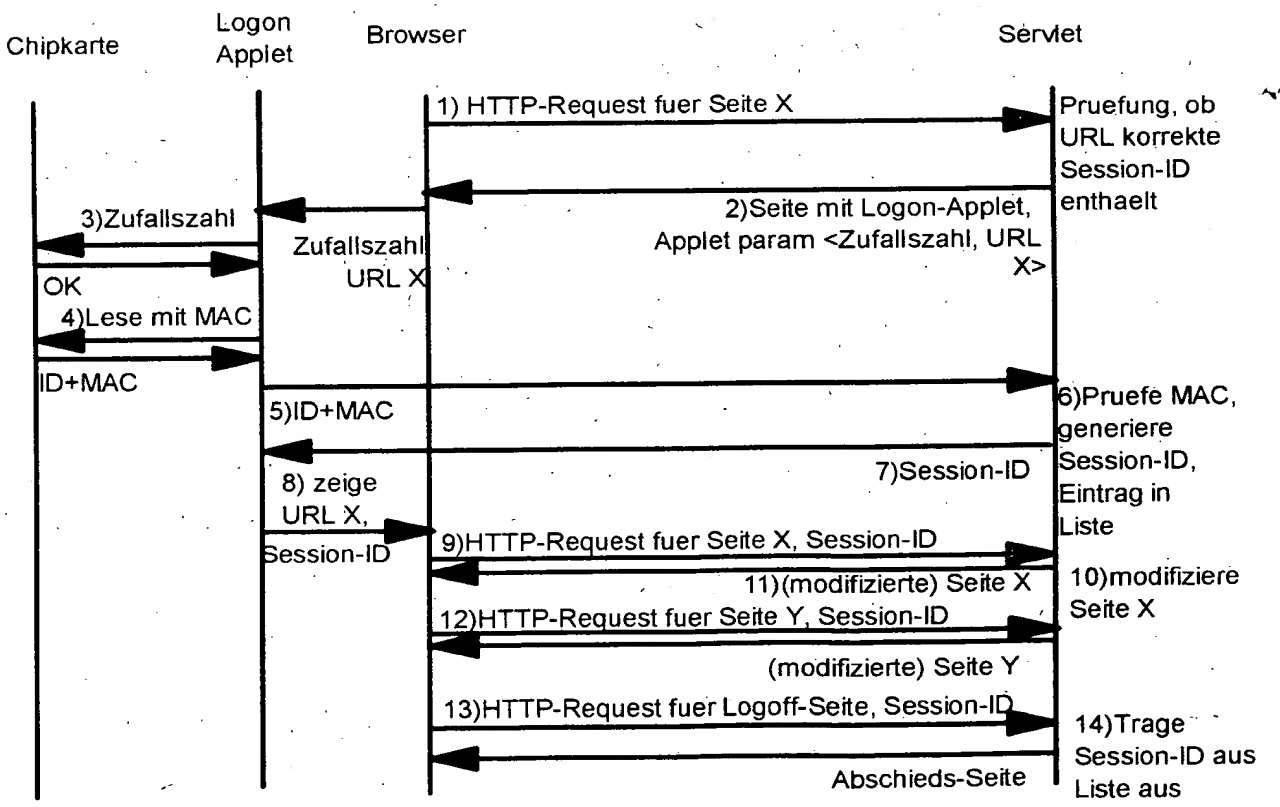
Chipkarte
Logon
Applet
Browser
Servlet
1) HTTP-Request fuer Seite X
Pruefung, ob
URL korrekte
Session-ID
enthaelt
2)Seite mit Logon-Applet,
Applet param <Zufallszahl, URL
X>
3)Zufallszahl
Zufallszahl
URL X
OK
4)Lese mit MAC
ID+MAC
5)ID+MAC
6)Pruefe MAC,
generiere
Session-ID,
Eintrag in
Liste
7)Session-ID
8) zeige
URL X,
Session-ID
9)HTTP-Request fuer Seite X, Session-ID
11)(modifizierte) Seite X
10)modifiziere
Seite X
12)HTTP-Request fuer Seite Y, Session-ID
(modifizierte) Seite Y
13)HTTP-Request fuer Logoff-Seite, Session-ID
14)Trage
Session-ID aus
Liste aus
Abschieds-Seite

FIG. 2